

Abstract Submitted  
for the MAR07 Meeting of  
The American Physical Society

**Decoy State Quantum Key Distribution: Theory and Practice**

YI ZHAO, Center for Quantum Information and Quantum Control, Department of Physics and Department of Electrical & Computer Engineering, University of Toronto, HOI-KWONG LO, XIONGFENG MA, BING QI, KAI CHEN, LI QIAN — Decoy state quantum key distribution (QKD) has been proposed as a novel approach to improve dramatically both the security and the performance of practical QKD set-ups. We proved its security, and proposed the first practical decoy state QKD protocols, including the one-decoy protocol, the weak+vacuum protocol, and the general two-decoy protocol. Our further study shows that the two-way communication can effectively improve the performance of decoy state QKD. We performed the first experiments of decoy state QKD. Two protocols – the one-decoy protocol and the weak+vacuum protocol – were implemented with a maximum transmission distance of 60km. We implemented the decoy state method by adding commercial acousto-optic modulator to a commercial QKD system. Our theoretical and experimental studies show explicitly the power and the feasibility of decoy method, and brings it to our real- life. Our works are published in [1-5]. [1] H. -K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. 94 230504 (2005) [2] X. Ma *et. al.*, Phys. Rev. A 72, 012326 (2005) [3] Y. Zhao *et. al.*, Phys. Rev. Lett., 96, 070502 (2006) [4] Y. Zhao *et. al.*, in *Proceedings of IEEE ISIT* (IEEE, 2006) pp. 2094-2098 [5] X. Ma *et. al.*, Phys. Rev. A 74, 032330 (2006)

Yi Zhao  
University of Toronto

Date submitted: 19 Nov 2006

Electronic form version 1.4